National Defense Industrial Association

16th Annual Security Technology Symposium

SECURITY RISK MANAGEMENT (SRM) PROGRAM

Quinten Johnson
Office of Civil Aviation Security
Policy & Planning

FAA INFRASTRUCTURE
The Long Pole In The Tent

- 49,000 PLUS PERMANENT EMPLOYEES
- 4,204 AIR NAVIGATION FACILITIES
  - EXAMPLES: VHF OMNI RANGE, INSTRUMENT LANDING SYSTEMS, APPROACH LIGHT SYSTEM, RUNWAY END IDENTIFICATION LIGHTS, AND RUNWAY VISUAL RANGE EQUIPMENT
- 3,685 AIR TRAFFIC CONTROL FACILITIES
  - EXAMPLES: AIR ROUTE TRAFFIC CONTROL CENTERS, AIRPORT TRAFFIC CONTROL TOWERS, AUTOMATED RADAR TERMINAL SYSTEMS, AND FLIGHT SERVICE STATIONS

WHAT IS SRM?

- **SRM is the logical process that is used to determine:**
  - **Criticality, vulnerability and risk**
  - **What risks are acceptable**
  - **What risks are unacceptable**
  - **What type and extent of countermeasures are required to reduce unacceptable risks to an acceptable level**
- **SRM is a dynamic and interactive process that should be part of the life cycle of every program, project, operation, system, and facility.**

DRIVERS

Common Sense & PDD-63

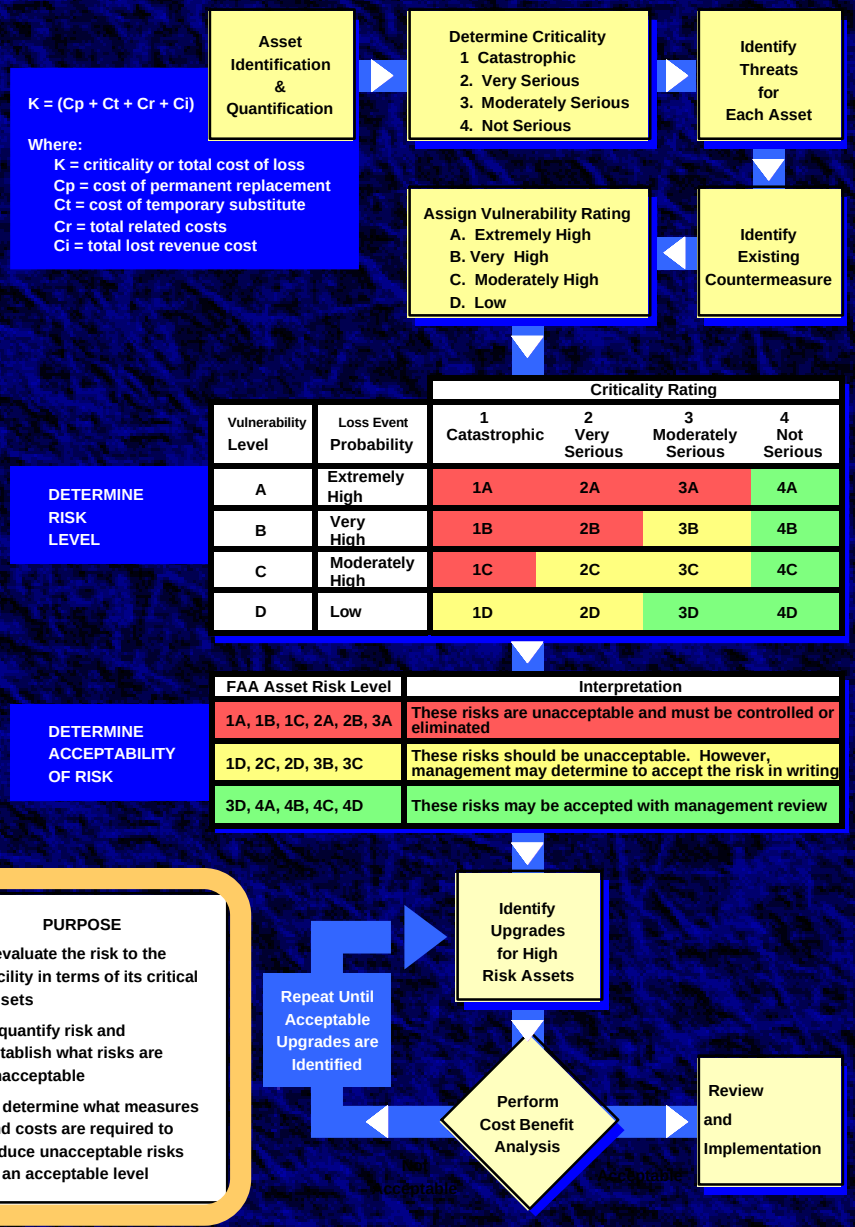
- **"...TO SWIFTLY ELIMINATE ANY SIGNIFICANT VULNERABILITY TO BOTH PHYSICAL AND CYBER ATTACKS ON OUR CRITICAL INFRASTRUCTURES.."** ***SRM DEVELOPS COST EFFECTIVE RISK REDUCTION COUNTER-MEASURES TO EFFECTIVELY ELIMINATE OR REDUCE VULNERABILITY AND RISKS TO FAA EMPLOYEES AND CRITICAL INFRASTRUCTURE TO AN ACCEPTABLE LEVEL***

DRIVERS

FAA POLICY

"For operational integrity, the FAA will apply comprehensive security risk management strategies **to identify and effectively deal with vulnerabilities and risks to people and facilities. In addition to physical security activities, the FAA's information security efforts will ensure the availability , integrity, and confidentiality of NAS operational data and systems."** ***Jane F. Garvey, Administrator, Federal Aviation Administration, Blueprint for NAS Modernization, January 1999***

FAA SECURITY RISK MANAGEMENT PROCESS



SRM Purpose

I. To evaluate the risk to the facility in terms of its critical assets

II. To quantify risk and establish what risks are unacceptable

III. To determine what measures and costs are required to reduce unacceptable risks to an acceptable level

FAA SECURITY RISK MANAGEMENT PROCESS

1 Asset Identification & Quantification

$K = (Cp + Ct + Cr + Ci)$

Where:
- K = criticality or total cost of loss
- Ci = initial asset cost
- Ct = cost of temporary substitute
- Cp = cost of permanent replacement
- Cr = IOL cost on all related systems

2 3 Determine Criticality
1. Catastrophic
2. Very Serious
3. Moderately Serious
4. Not Serious

4 Identify Threats for Each Asset

5 Identify Existing Countermeasure

6 Assign Vulnerability Rating
A. Extremely High
B. Very High
C. Moderately High
D. Low

7 DETERMINE RISK LEVEL

Vulnerability Level	Loss Event Probability	Criticality Rating: 1 Catastrophic	2 Very Serious	3 Moderately Serious	4 Not Serious
A	Extremely High	1A	2A	3A	4A
B	Very High	1B	2B	3B	4B
C	Moderately High	1C	2C	3C	4C
D	Low	1D	2D	3D	4D

8 DETERMINE ACCEPTABILITY OF RISK

FAA Asset Risk Level	Interpretation
1A, 1B, 1C, 2A, 2B, 3A	These risks are unacceptable and must be controlled or eliminated
1D, 2C, 2D, 3B, 3C	These risks should be unacceptable. However, management may determine to accept the risk in writing
3D, 4A, 4B, 4C, 4D	These risks may be accepted with management review

9 Identify Upgrades for High Risk Assets

Repeat Until Acceptable Upgrades are Identified

10 Perform Cost Benefit Analysis

Not Acceptable

Acceptable

11 Final Management Review

PURPOSE

I. To evaluate the risk to the facility in terms of its critical assets

II. To quantify risk and establish what risks are unacceptable

III. To determine what measures and costs are required to reduce unacceptable risks to an acceptable level

SRM Review

1. Asset Identification and Quantification
2. Determine Criticality Rating
3. Assign Criticality Designator
4. Identify Threats to Each Asset
5. Identify Existing Countermeasure
6. Assign Vulnerability Level
7. Determine Risk Level
8. Determine Acceptability of Risk
9. Identify Risk Reduction Measures
10. Perform Cost Benefit Analysis
11. Review and Implementation

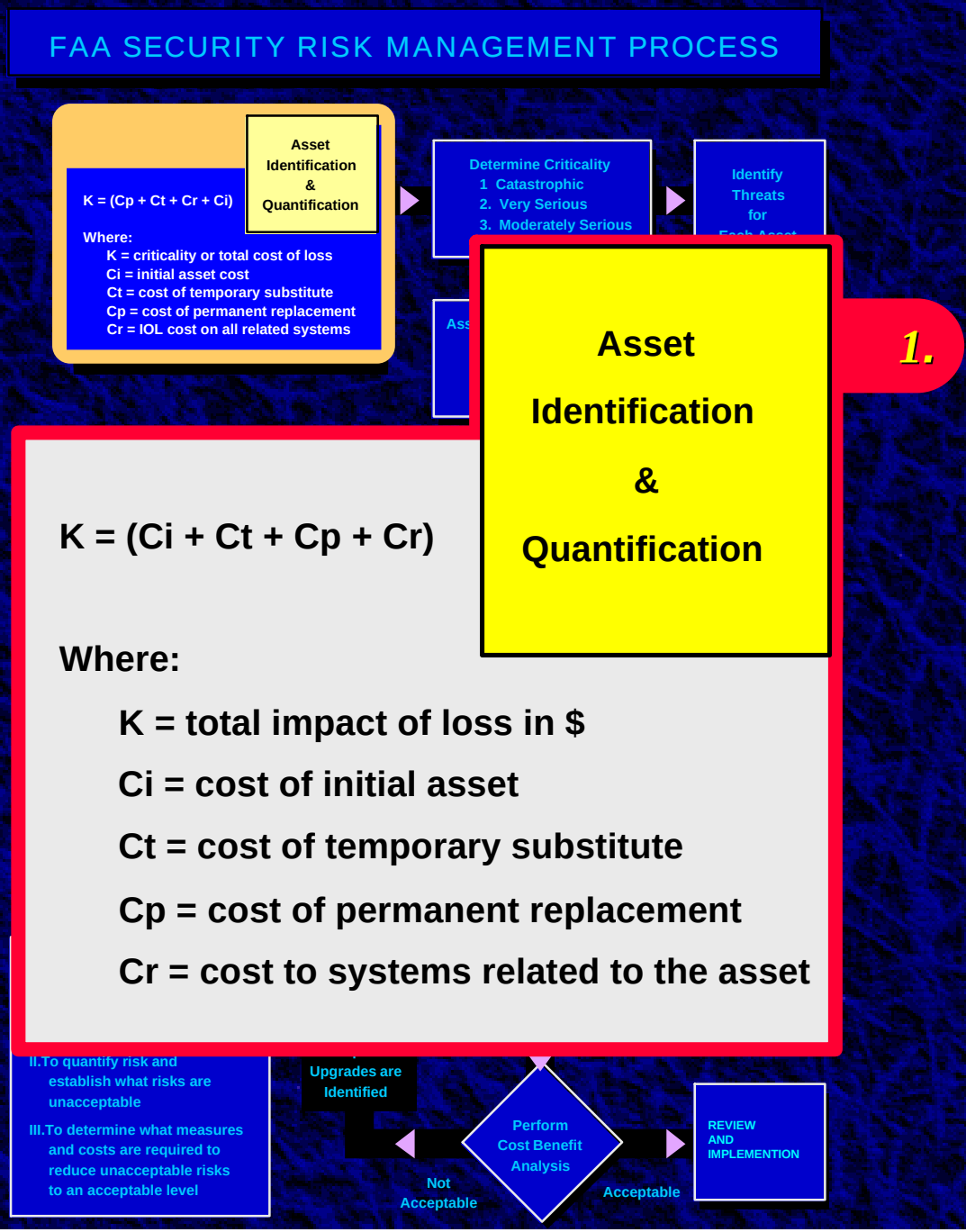
IDENTIFICATION OF ASSETS

- **It is essential that the critical assets be identified and quantified to develop a true perspective regarding criticality and impact of loss.**

- **In terms of the common language of SRM, human life must be assigned a value as the most critical of FAA's assets. This value is $2.7 million per human life.**

CONCEPT OF ASSET

- **Assets include personnel, equipment, systems, operations, data, and procedures, whose value can be quantified in terms of dollars.**
- **Each asset can have vulnerabilities and risks.**
- **To evaluate pure risk, assets must be quantified in terms of criticality, vulnerability, and risk.**



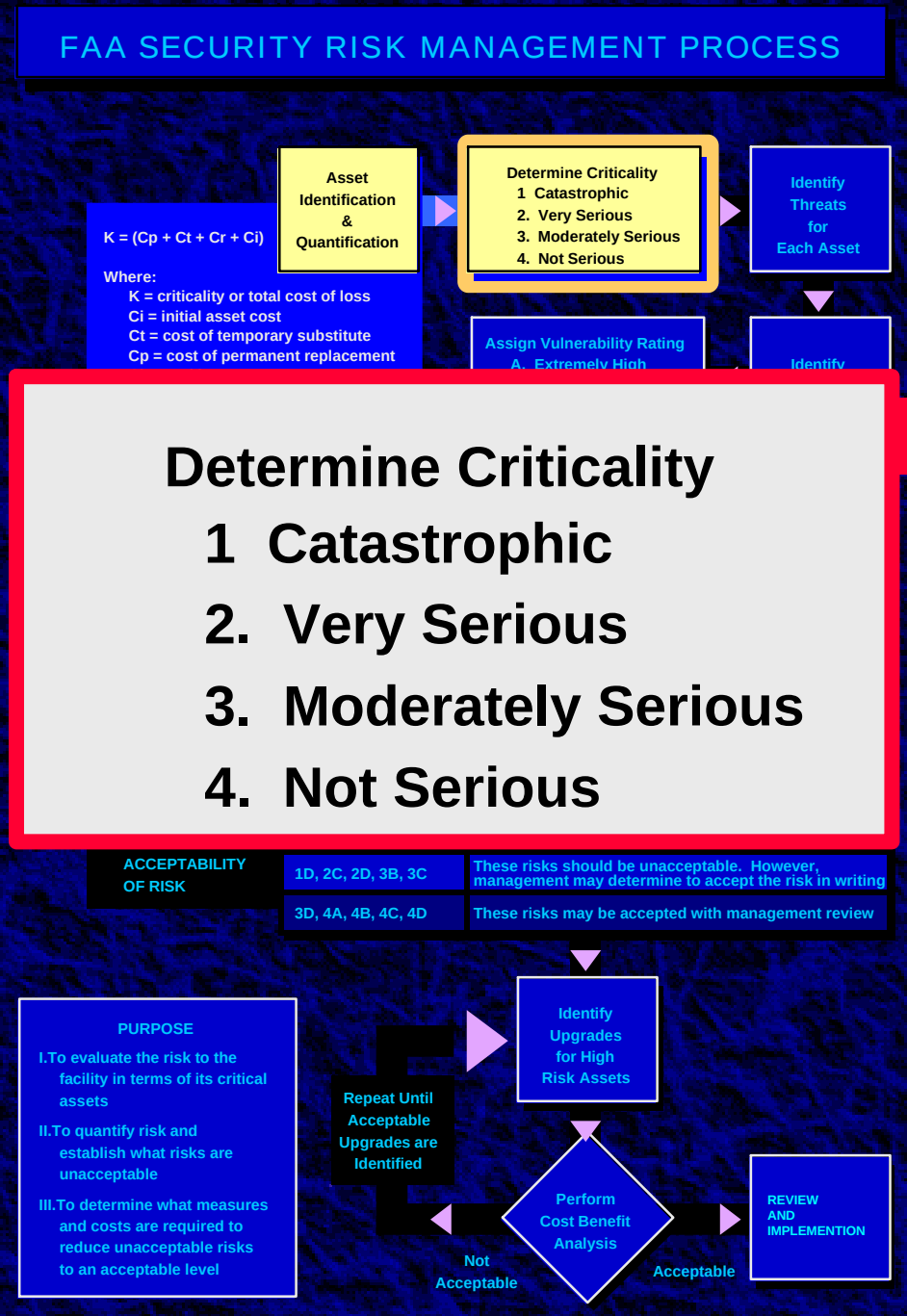
SRM Asset Identification

Identification of assets

- Assets are specifically identified by function and criticality
- Each asset is evaluated in $ cost terms of its:
  - Initial acquisition
  - Temporary substitute
  - Permanent replacement
  - Related systems impacted by the asset's loss

INDEX

SRM Determine Criticality



3. **Assign a numeric criticality designator.**

Arrange assets in order of priority with the most critical first, and the least critical last.

FAA SECURITY RISK MANAGEMENT PROCESS

SRM Risk Logic

Asset Identification & Quantification

Determine Criticality
1. Catastrophic
2. Very Serious
3. Moderately Serious
4. Not Serious

Identify Threats for Each Asset

Identify Existing Countermeasure

Assign Vulnerability Rating
A. Extremely High
B. Very High
C. Moderately High
D. Low

$K = (Cp + Ct + Cr + Ci)$

Where:
- K = criticality or total cost of loss
- Ci = initial asset cost
- Ct = cost of temporary substitute
- Cp = cost of permanent replacement
- Cr = IOL cost on all related systems

RISK MATRIX

Vulnerability Level	Loss Event Probability	Criticality Rating: 1 Catastrophic	2 Very Serious	3 Moderately Serious	4 Not Serious
A	Extremely High	1A	2A	3A	4A
B	Very High	1B	2B	3B	4B
C	Moderately High	1C	2C	3C	4C
D	Low	1D	2D	3D	4D

BUY IN

- Facility Manager
- Facility Security Risk Management Committee
- Associate Administrator for Air Traffic Services
- Joint Resources Council
- Administrator

BUY WHAT?

- **Funding Stream Is Baselined**
  - **NAS Facilities Program Decides**
    - **Integrated Product Team Buys**

BUY WHAT?

- Funding Stream Is Baselined
  - NAS Facilities Program Decides
    - Integrated Product Team Buys

EVERYBODY GRIPES !

For more information, contact:

David C. McFadden, CPP
202-366-0985
david.mcfadden@faa.gov

National Defense Industrial Association

16th Annual Security Technology Symposium

SECURITY RISK MANAGEMENT (SRM) PROGRAM

Quinten Johnson
Office of Civil Aviation Security
Policy & Planning